

2007 ACSA Conference Work In Progress Abstract Submission

Title: *Towards a High Assurance, Multi-level Secure, Off-the-Shelf PC*

Presenter: David Kleidermacher, Chief Technology Officer, Green Hills Software, Inc.

Military and intelligence communities have long struggled with the burden of maintaining separate computers and networks to manage information at varying security levels. Commercial grade operating systems and virtualization solutions such as Windows, Linux, and VMware are unsuitable for security assurance to the high levels required for this kind of information sharing on a single PC platform. Custom solutions have failed to gain acceptance as cost containment pressures favor commercial, off-the-shelf (COTS) platforms. In addition, common PC hardware has had serious security limitations that prevent even a high assurance software solution from achieving the required domain separation. The hope for a truly high assurance, multi-level secure PC is coming closer to reality by virtue of recent innovations, both in software and hardware.

On the software side is INTEGRITY PC: an operating environment based on the safety-certified INTEGRITY real-time operating system and incorporating a suite of secure software components, including virtualization software (called Padded Cell™). Padded Cell enables multiple guest operating systems – such as Windows, Linux, and Solaris – and their applications to be run in secure partitions on the same computer. Because INTEGRITY itself is a full-featured operating system, secure native applications, such as regraders and audit log reviewers, can be developed to run alongside familiar PC operating environments. A multi-level secure PC saves cost, size, weight, and power over multiple hardware platforms (figure 1).

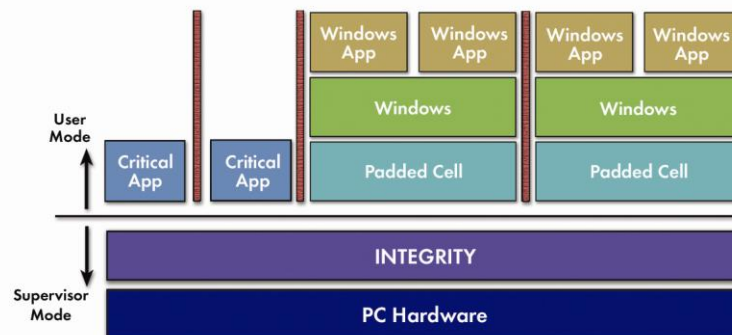


Figure 1 - INTEGRITY PC architecture

INTEGRITY provides the assured separation between INTEGRITY PC's guest operating environments and critical applications, including the kernel itself. INTEGRITY is currently undergoing the first ever high assurance (EAL 6+) Common Criteria security evaluation (http://www.niap-ccevs.org/cc-scheme/in_evaluation.cfm; validation id 10119).

On the hardware side, Intel and AMD have been adding important features to their chips and chipsets which aid in both virtualization and platform security. INTEGRITY PC takes advantage of Intel VT-x technology to accelerate the performance of the virtualization components. In August 2007, Intel announced its latest vPro™ chipsets which add Intel TXT and VT-d technologies which enable secure boot and attestation as well as protection against rogue peripherals. Inability to

guarantee a secure initial state and protect against untrusted peripherals have been major roadblocks in meeting multi-level security requirements on commodity PC platforms. Support for these hardware features is being incorporated into INTEGRITY PC.

A true multi-level secure workstation requires a multi-level secure window manager, cross-domain information transfer framework, shared keyboard and mouse drivers, and a multi-factor authentication mechanism. Each of these components manages information at multiple security levels and hence must meet high assurance requirements. INTEGRITY PC incorporates these software components.

INTEGRITY PC has been tested, demonstrated, and deployed at several advanced technology concerns within the military and military contractors.

Work In Progress

In our session, we will provide a brief overview of the multi-level secure PC effort and status on the following works in progress: high assurance kernel evaluation, multi-level component development, and secure boot and attestation. We will identify the major problems and challenges that remain on both the software and hardware sides. We will also provide a summary of results to be published prior to the date of the ACSA conference regarding the use of INTEGRITY PC in a recent CWID - Coalition Warrior Interoperability Demonstration.